Claims

What is claimed is:

Sub A4

1. An extremely secure method for a host processor to key a source content to a source storage medium to prevent use of an unauthorized copy of the source content comprising the host processor storing a fingerprinted content comprising the steps of:

determining a source fingerprint from the source storage medium;

combining the content to be secured with the source fingerprint to generate the fingerprinted content; and

instructing the source medium to store the fingerprinted content.

2. The extremely secure method of Claim 1 further comprising the step of a processor reading and verifying the fingerprinted content, the reading and verifying step comprising the steps of:

instructing a local storage medium to read the fingerprinted content;

separating the content to be secured from the source fingerprint;

requesting a local fingerprint from the local medium; and

comparing the local fingerprint with the source fingerprint and in response to the comparison determining whether to use the source content.

3. The extremely secure method of Claim 2 wherein the step of requesting a source fingerprint further comprises:

using an open protocol to request a secured communication from the source medium;

identifying a physical, statistically unique, verifiable and relatively immutable characteristic (PSUVI) associated with the source medium;

generating at least one of encryption and decryption keys;

returning the encryption key to the host processor;

using the encryption key to convert the source content to an encrypted protocol;

requesting from the source medium the PSUVI fingerprint characteristic; and

the source medium responding to the host processor with the PSUVI fingerprint.

4. The extremely secure method of Claim 2 wherein the step of combining the source content with the source fingerprint to generate the fingerprinted source contents further comprises:

creating a hybrid content to be secured by combining the content to be secured and the source fingerprint; and

encrypting the fingerprinted source content with an encryption key.

5. The extremely secure method of Claim 2 wherein the step of requesting a local fingerprint from the local storage medium further comprises the steps of:

requesting from the local storage medium a local fingerprint PSUVI characteristic;

replying to the host processor with the local fingerprint PSUVI; and

performing a secured verification of the local fingerprint PSUVI.

6. The extremely secure method of Claim 2 wherein the step of requesting a source fingerprint further comprises:

using an open protocol to request a secured communication from the source medium;

identifying a relatively mutable physical attribute (Non-PSUVI) associated with the source medium;

generating at least one of encryption and decryption keys;

returning the encryption key to the host processor;

using the encryption key to convert the source content to an encrypted protocol;

requesting from the source medium the non-PSUVI fingerprint characteristic; and

the source medium responding to the host processor with the non-PSUVI fingerprint.

7. The extremely secure method of Claim 2 wherein the step of requesting a local fingerprint from the local storage medium further comprises the steps of:

requesting from the local storage medium a local fingerprint non-PSUVI characteristic;

replying to the host processor with the local fingerprint non-PSUVI; and

performing a secured verification of the local fingerprint non-PSUVI.

8. An extremely secure system to prevent use of an unauthorized copy of a source content on a storage medium comprising:

a host processor; and

a storage medium, the storage medium comprising a storage medium processor, a host processor interface, a servo system, a read/write system, one or more storage disks, and an attribute detector to read a PSUVI characteristic from the one or more storage disks to use by the host processor to encrypt a content to be secured.

9. An extremely secure system to prevent use of an unauthorized copy of a source content on a storage medium comprising:

a host processor; and

a storage medium, the storage medium comprising a storage medium processor, a host processor interface, a servo system, a read/write system, one or more storage disks, and an attribute detector to read a non-PSUVI characteristic from the one or more storage disks to use by the host processor to encrypt a content to be secured.

10. An extremely secure fingerprinted content of a storage medium, wherein the fingerprinted content comprises a content to be secured combined with a fingerprint generated from a PSUVI characteristic of the storage medium.

11. An extremely secure fingerprinted content of a storage medium, wherein the fingerprinted content comprises a content to be secured combined with a fingerprint generated from a non-PSUVI characteristic of the storage medium.

5

Add A5